

1 CLAIMS

2

3 WHAT IS CLAIMED IS:

4

5 1. A method of secure information distribution between
6 nodes, the method comprising:

7 performing a handshake process with an adjacent node

8 to determine membership in a secure group; and

9 distributing secure information to the adjacent node,

10 if the adjacent node is a member of the secure group.

11

12 2. The method of claim 1, further comprising:

13 prior to providing the secure information to the
14 adjacent node, performing the handshake process with
15 another adjacent node.

16

17 3. The method of claim 1, further comprising:

18 establishing an encryption key with the adjacent node.

19

20 4. The method of claim 3, wherein the encryption key
21 comprises a public key.

22

23 5. The method of claim 3, wherein the encryption key
24 comprises a symmetric key.

1

2 6. The method of claim 3, wherein the secure information
3 is distributed along with an encryption key.

4

5 7. The method of claim 1, wherein the action of
6 performing the handshaking process comprises:

7 using a one way function $f(x)$ to determine if the
8 adjacent node is a member of the secure group.

9

10 8. The method of claim 7, wherein the one way function
11 $f(x)$ is a secure hash function.

12

13 9. The method of claim 1, wherein the action of
14 performing the handshaking process comprises:

15 providing, by a first node, a component value A_1 for a
16 one way function $f(x)$;

17 providing, by the adjacent node, a component value B_1
18 as a challenge to the first node; and

19 applying the component values A_1 and B_1 , and a key
20 value SGK to the one way function $f(x)$ to generate a value
21 y .

22

23 10. The method of claim 9, wherein the one way function
24 $f(x)$ is a secure hash function.

1

2 11. The method of claim 1, wherein the secure information
3 comprises a password.

4

5 12. The method of claim 1, wherein the secure information
6 comprises a key for secure communication.

7

8 13. The method of claim 1, further comprising:
9 distributing secure information to each adjacent node
10 that is a member of the secure group, in response to an
11 update of the secure information.

12

13 14. The method of claim 1, wherein the action of
14 performing the handshake process comprises:

15 performing the handshake process with the adjacent
16 node once for every fixed time amount T.

17

18 15. The method of claim 1, further comprising:
19 after detecting the presence of another node that is
20 not in an adjacency set, attempting to handshake with that
21 another node if a detecting node and the another node both
22 have a handshake time remaining value of zero (0).

23

24 16. The method of claim 1, further comprising:

1 determining an age of the secure information so that
2 each node in the secure group will store a latest version
3 of the secure information.

4

5 17. The method of claim 16, wherein the action of
6 determining the age of the secure information comprises:

7 checking a sequence number of the secure information
8 to determine the age of the secure information.

9

10 18. The method of claim 16, wherein the action of
11 determining the age of the secure information comprises:
12 checking a date of modification of the secure
13 information to determine the age of the secure information.

14

15 19. The method of claim 16, wherein the action of
16 determining the age of the secure information comprises:
17 checking an elapsed time since a previous modification
18 of the secure information to determine the age of the
19 secure information.

20

21 20. The method of claim 1, further comprising:
22 resolving an ambiguity between a received updated
23 secure information and currently stored secure information

1 by selecting the secure information with a larger data
2 value.

3

4 21. The method of claim 1, further comprising:
5 increasing a security of the secure group by widening
6 a secure group key (SGK) value which is known by each node
7 in the secure group.

8

9 22. The method of claim 1, further comprising:
10 decreasing an amount of time between symmetric key
11 regeneration (TK) to increase the security of the secure
12 group.

13

14 23. The method of claim 1, further comprising:
15 allowing for rapid construction of the secure group by
16 transmitting a burst of NB handshakes for every amount of
17 time TB, where NB is the number of handshakes and TB is a
18 time amount between burst of handshakes.

19

20 24. The method of claim 1, further comprising:
21 preventing a single node in the secure group from
22 attempting to handshake with numerous nodes to avoid
23 excessive joins, by establish membership with one adjacent
24 node at a time, and waiting at time TW + TR between

1 handshake attempts, where TW is a fixed configurable time
2 amount and TR is a random amount of time that is bounded by
3 a user-specified bound range.

4

5 25. An apparatus for secure information distribution
6 between nodes, the apparatus comprising:

7 a node configured to performing a handshake process
8 with an adjacent node to determine membership in a secure
9 group, and distribute secure information to the adjacent
10 node, if the adjacent node is a member of the secure group.

11

12 26. The apparatus of claim 25, wherein the node performs
13 the handshake process with another adjacent node, prior to
14 providing the secure information to the adjacent node.

15

16 27. The apparatus of claim 25, wherein the node is
17 configured to establish an encryption key with the adjacent
18 node.

19

20 28. The apparatus of claim 25, wherein the encryption key
21 comprises a public key.

22

23 29. The apparatus of claim 25, wherein the encryption key
24 comprises a symmetric key.

1

2 30. The apparatus of claim 27, wherein the secure
3 information is distributed along with an encryption key.

4

5 31. The apparatus of claim 25, wherein the node is
6 configured to use a one way function $f(x)$ to determine if
7 the adjacent node is a member of the secure group.

8

9 32. The apparatus of claim 31, wherein the one way
10 function $f(x)$ is a secure hash function.

11

12 33. The apparatus of claim 25, wherein the node is
13 configured to provide a component value A_1 for a one way
14 function $f(x)$, and wherein the adjacent node is configured
15 to provide a component value B_1 as a challenge to the first
16 node; and wherein the node and adjacent node are configured
17 to apply the component values A_1 and B_1 , and a key value
18 SGK to the one way function $f(x)$ to generate a value y .

19

20 34. The apparatus of claim 33, wherein the one way
21 function $f(x)$ is a secure hash function.

22

23 35. The apparatus of claim 25, wherein the secure
24 information comprises a password.

1

2 36. The apparatus of claim 25, wherein the secure
3 information comprises a key for secure communication.

4

5 37. The apparatus of claim 25, wherein the node is
6 configured to distribute the secure information to each
7 adjacent node that is a member of the secure group, in
8 response to an update of the secure information.

9

10 38. The apparatus of claim 25, wherein the node is
11 configured to perform the handshake process with the
12 adjacent node once for every fixed time amount T.

13

14 39. The apparatus of claim 25, wherein the node is
15 configured to attempt to handshake with another node if the
16 node and the another node both have a handshake time
17 remaining value of zero (0).

18

19 40. The apparatus of claim 25, wherein the node is
20 configured to determine an age of the secure information so
21 that each node in the secure group will store a latest
22 version of the secure information.

23

1 41. The apparatus of claim 25, wherein the node is
2 configured to check a sequence number of the secure
3 information to determine the age of the secure information.

4

5 42. The apparatus of claim 25, wherein the node is
6 configured to check a date of modification of the secure
7 information to determine the age of the secure information.

8

9 43. The apparatus of claim 25, wherein the node is
10 configured to check an elapsed time since a previous
11 modification of the secure information to determine the age
12 of the secure information.

13

14 44. The apparatus of claim 25, wherein the node is
15 configured to resolve an ambiguity between a received
16 updated secure information and currently stored secure
17 information by selecting the secure information with a
18 larger data value.

19

20 45. The apparatus of claim 25, wherein the node is
21 configured to increase a security of the secure group by
22 widening a secure group key (SGK) value which is known by
23 each node in the secure group.

24

1 46. The apparatus of claim 25, wherein the node is
2 configured to decrease an amount of time between symmetric
3 key regeneration (TK) to increase the security of the
4 secure group.

5

6 47. The apparatus of claim 25, wherein the node is
7 configured to allow for rapid construction of the secure
8 group by transmitting a burst of NB handshakes for every
9 amount of time TB, where NB is the number of handshakes and
10 TB is a time amount between burst of handshakes.

11

12 48. The apparatus of claim 25, wherein the node is
13 prevented from attempting to handshake with numerous nodes
14 to avoid excessive joins, by establish membership with one
15 adjacent node at a time, and waiting at time $TW \pm TR$
16 between handshake attempts, where TW is a fixed
17 configurable time amount and TR is a random amount of time
18 that is bounded by a user-specified bound range.

19

20 49. An apparatus for secure information distribution
21 between nodes, the apparatus comprising:

22 means for performing a handshake process with an
23 adjacent node to determine membership in a secure group;
24 and

1 means for distributing secure information to the
2 adjacent node, if the adjacent node is a member of the
3 secure group.

4

5 50. An article of manufacture, comprising:

6 a machine-readable medium having stored thereon
7 instructions to:

8 perform a handshake process with an adjacent node to
9 determine membership in a secure group; and
10 distribute secure information to the adjacent node, if
11 the adjacent node is a member of the secure group.